Cisco Next Gen SD-WAN

Webinar 17 July 2018

Cisco SDWAN

Powered by Cisco Digital Network Architecture

Ronald Tan

Regional Sales Director

Enterprise Networking Sales

17 July 2018

What is SDWAN?

- Unified Threat Management?
- Link Diversity?
- Connectivity?

Second Wave of SDN Is Coming to the WAN

Apps are moving to the cloud
80/20 now becomes 20/80

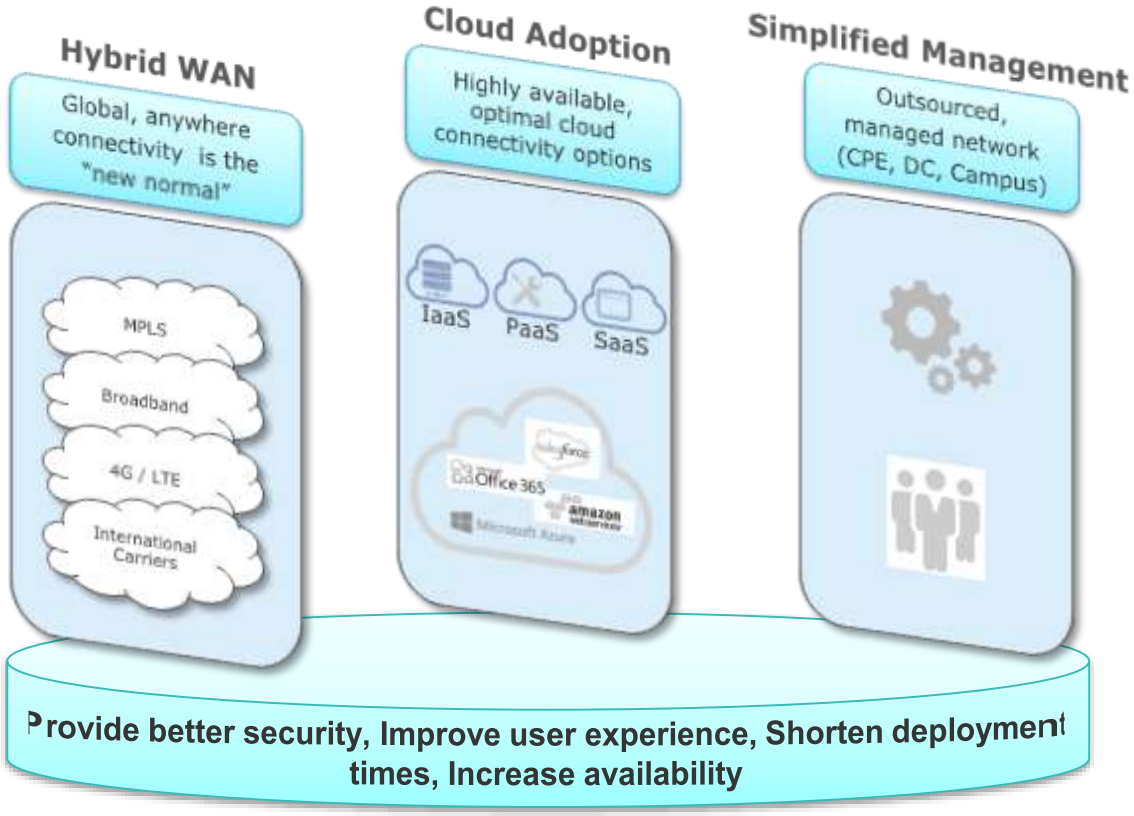
Mobile/IoT device proliferation
Collaboration
QoS

Internet edge moving to the branch
More requirements for security

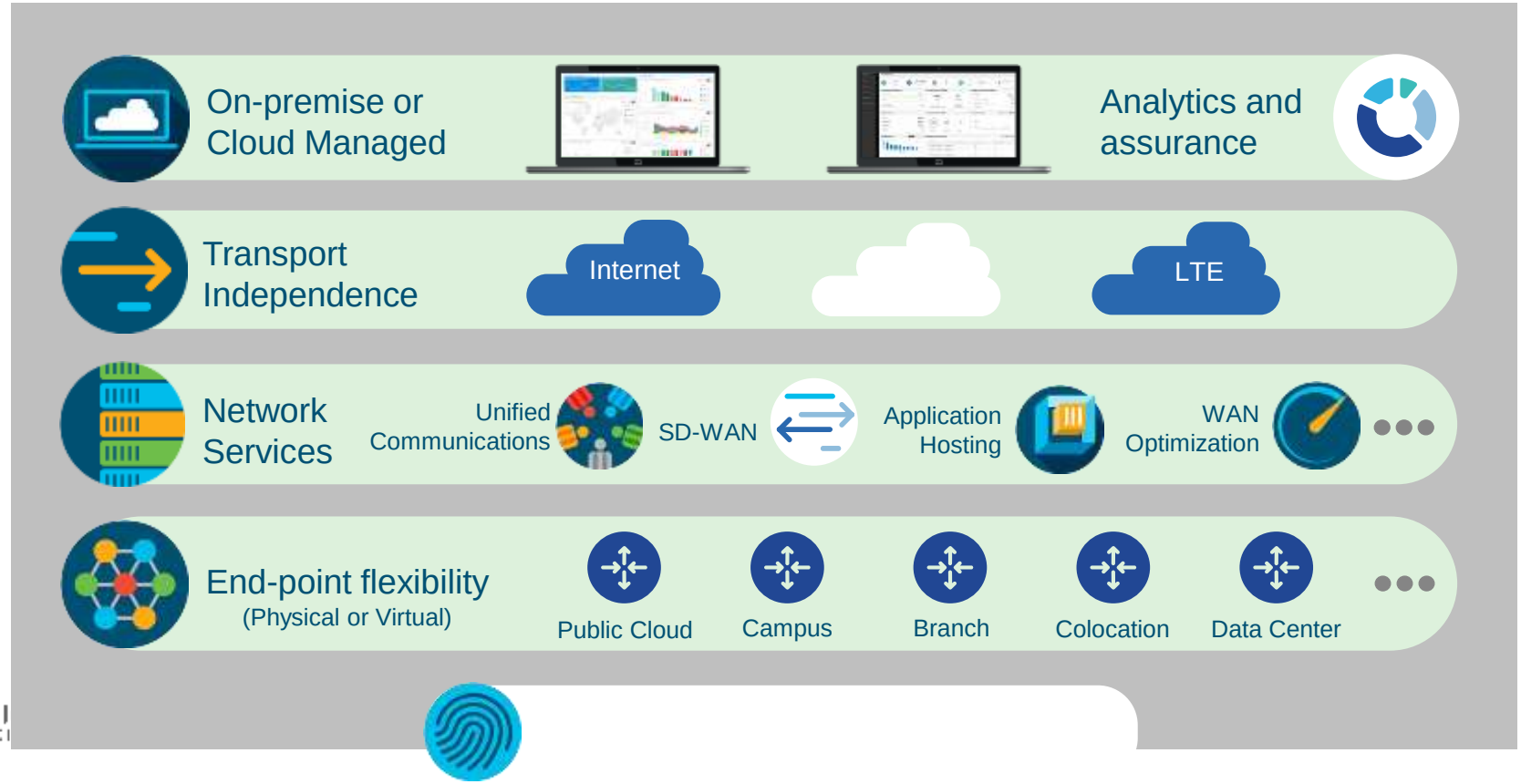
Managing the network is getting more complex

Today's WAN Challenges

What Enterprise Customers Are Asking For?



Cisco SDWAN Architecture



Spend less time troubleshooting WAN issues

End-to-end visibility

- 360-degree view across network
- Historical view
- Ability to follow the network path

Proactive and predictive insights

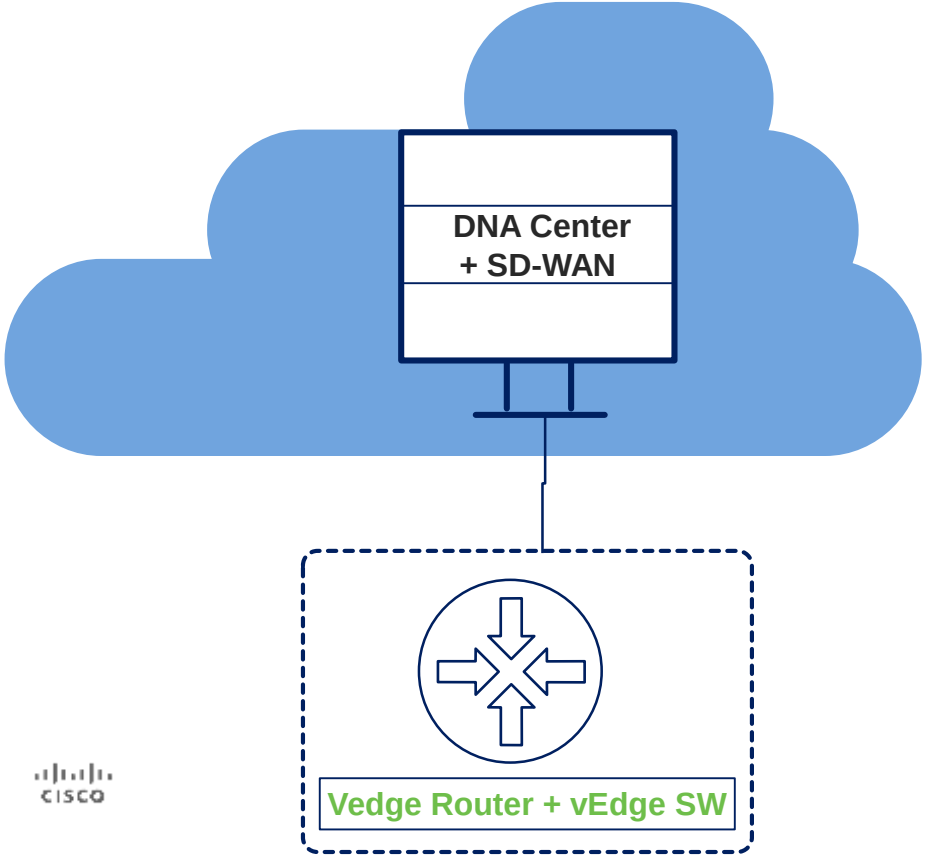
- Proactive to get ahead of the problem
- Predictive to stay ahead
- Assessment to see impact of changes

Guided remediation

- Today: Remediate with user input
- Future: Automated remediation

Transform WAN Operations with actionable insights

Market Leading Routing + SD WAN



Leading Routing &
SD-WAN Platforms

CISCO

+

Cloud-managed &
Feature-rich SD-WAN

viptela

Cisco SD-WAN Platform Options

Branch Services

ISR 1000

- 200 Mbps
- Next-gen connectivity
- Performance flexibility

ISR 4000

- Up to 2 Gbps
- Modular
- Integrated service containers
- Compute with UCS E

ASR 1000

- 2.5-200Gbps
- High-performance service w/hardware assist
- Hardware & software redundancy

vEdge Appliances

vEdge 100

- 100 Mbps
- 4G LTE & Wireless

vEdge 1000

- Up to 1 Gbps
- Fixed

vEdge 2000/5000

- 10 to 20 Gbps
- Modular

Simplified SDWAN Cloud

cisco Meraki

Virtualization

ENCS 5100

- Up to 250Mbps

ENCS 5400

- 250Mbps – 2GB

Public Cloud

Microsoft Azure

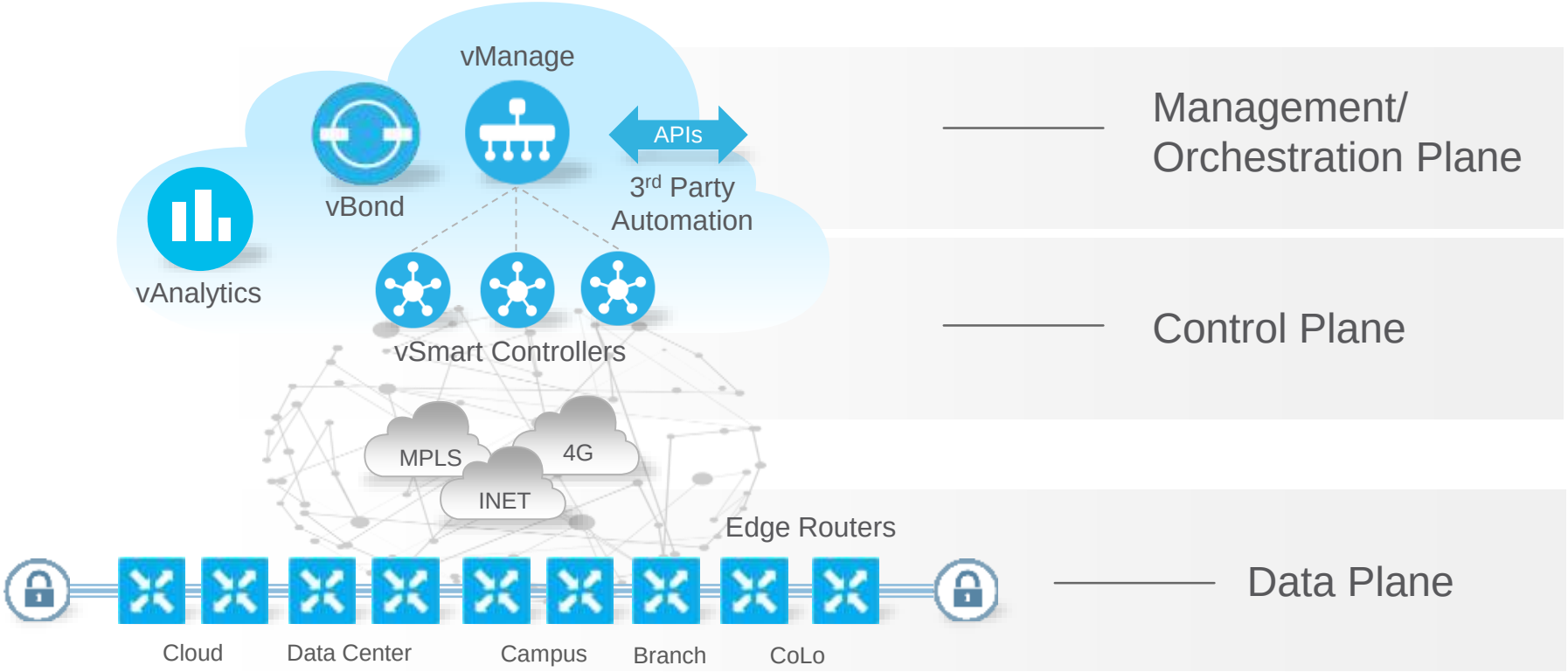
amazon web services

Cisco SD-WAN (Viptela)

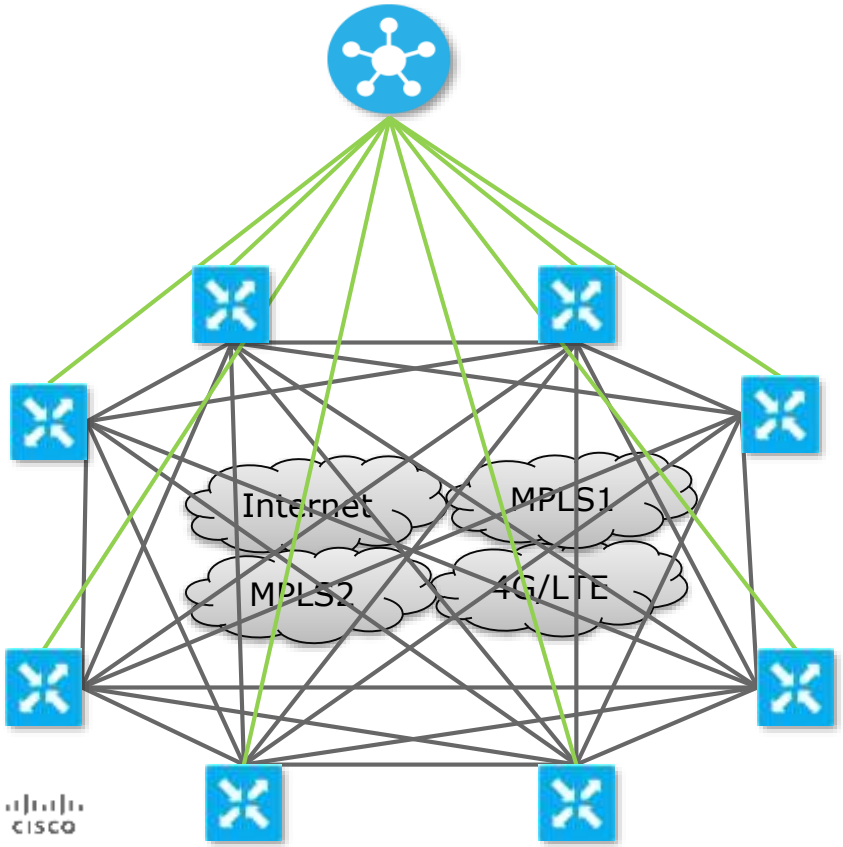
Next-Gen Cisco SD-WAN Architecture

Shamil Fernando
Manager System Engineering (APAC & Japan)
shamilf@cisco.com

Cisco SD-WAN Solution Principals

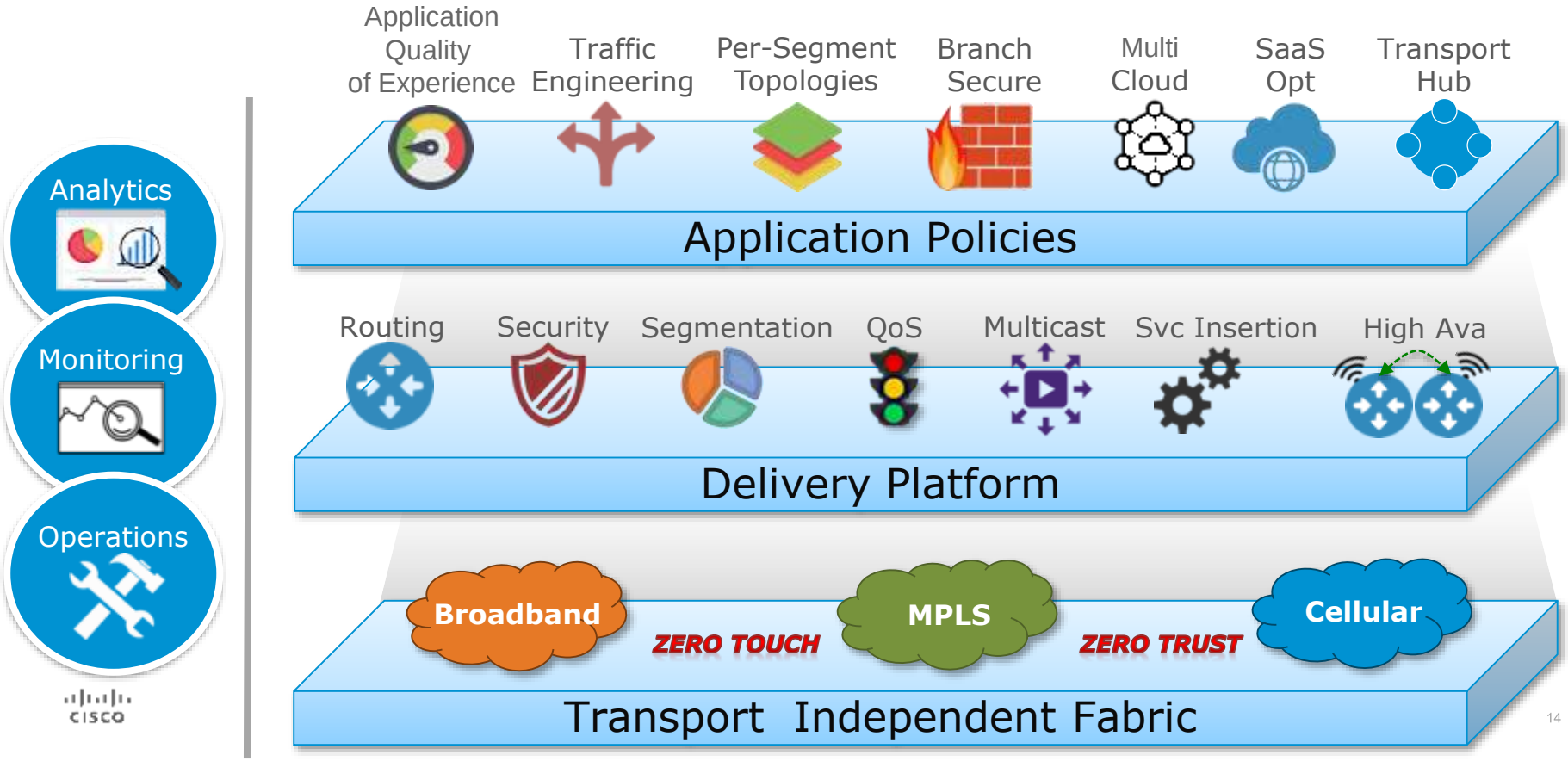


Cisco SD-WAN Solution Principals



- Separation Control and Data Plane
- DTLS/TLS is used to establish the control channel
- Control channel is established only with central controllers
- No scaling issues are with full mesh of control plane
- Control channel does not have to follow the data path

Cisco SD-WAN Solution



Cisco SD-WAN Edge Devices

18th July 2018

Branch Services

ISR 1000

- 200 Mbps
- Next-gen connectivity
- Performance flexibility

ISR 4000

- Up to 2 Gbps
- Modular
- Integrated service containers
- Compute with UCS E

ASR 1000

- 2.5-200Gbps
- High-performance service w/hardware assist
- Hardware & software redundancy

SD-WAN

vEdge 100

- 100 Mbps
- 4G LTE & Wireless

vEdge 1000

- Up to 1 Gbps
- Fixed

vEdge 2000

- 10 Gbps
- Modular

vEdge 5000

- 20 Gbps
- Modular

Virtualization

ENCS 5100

- Up to 250Mbps

ENCS 5400

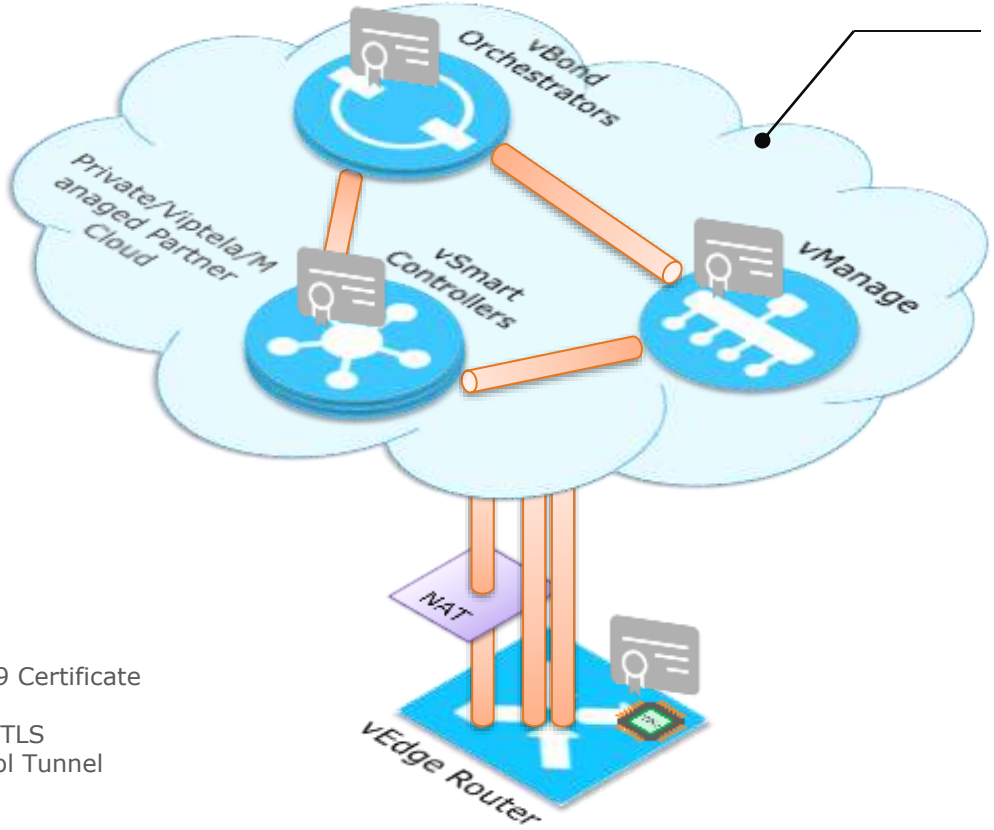
- 250Mbps – 2GB

Private / Public Cloud

Microsoft Azure

amazon web services

Zero-Trust Security Principles



Control Elements

X.509 Certificate

DTLS/TLS
Control Tunnel

- Strong authentication
  - PKI certificates, 2048bit keys
- Highly encrypted tunnels
  - DTLS/TLS AES256
  - White-list model
- Ubiquitous Deployment
  - Automatic NAT mitigation

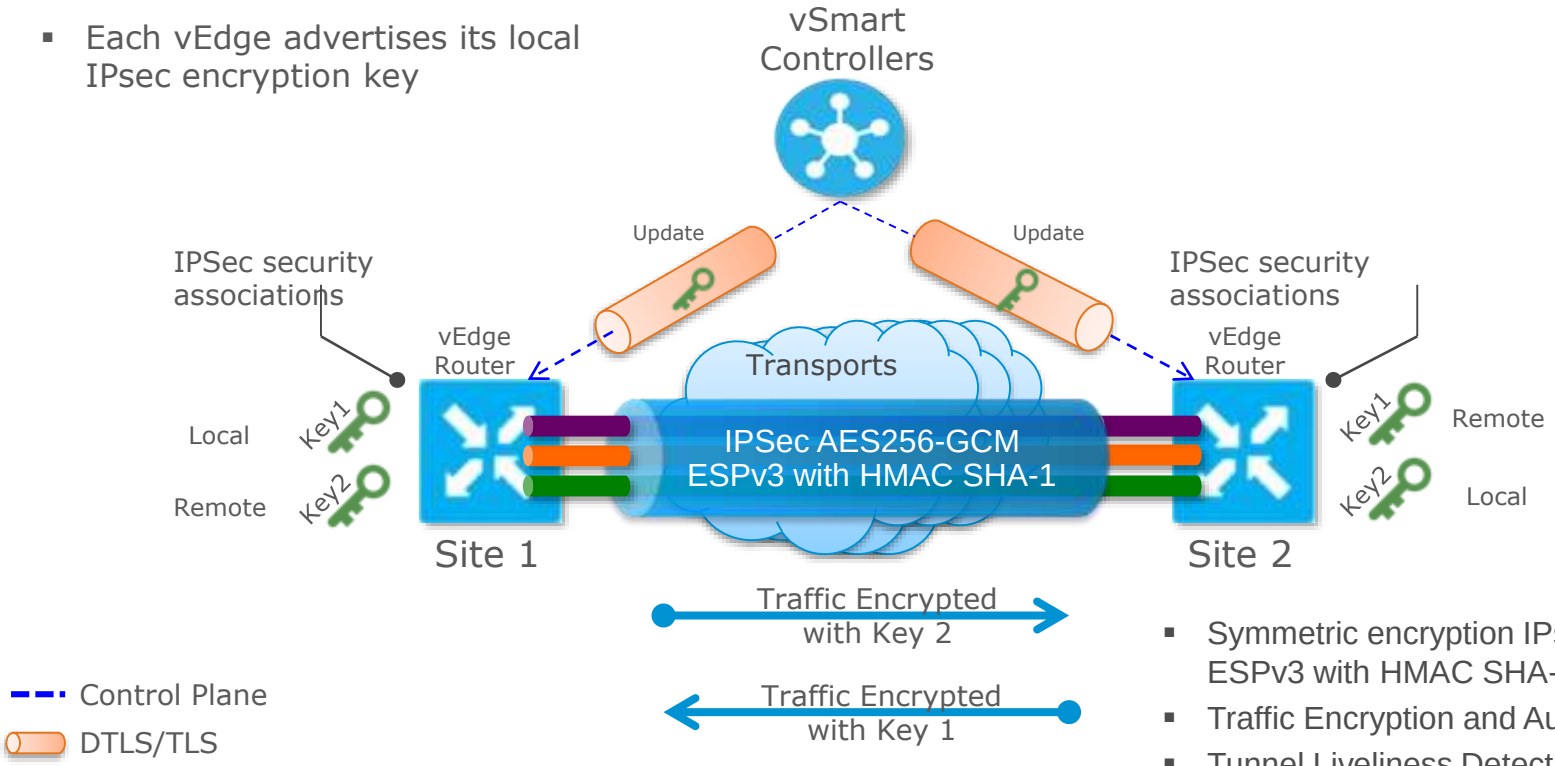
Secure Bring-up With Approval

Chassis Number	Certificate Serial	Hostname	IP Address	Validate ↓
9391da23-f0d1-4259..	0334D73E5EC036F87ABE...	DataCenter	1.1.1.5	invalid | staging | valid
4de0b85f-a2ae-42ec...	585A0084DEA8396DD77B..	RemoteSite	1.1.1.4	invalid | staging | valid
5f05358a-bef7-4e15...	248792F938E6EA8BEE6FD..	AWS	1.1.1.6	invalid | staging | valid

- Per-device control on TPM identity trust
- Single stage (Zero Touch Provisioning) – TPM identity is automatically trusted
- Two stage (One Touch Provisioning) – TPM identity is not automatically trusted. Requires administrator validation.
- Staging Mode – TPM identity is automatically trusted for control, but not for data. Requires administrator validation.

End to End Security

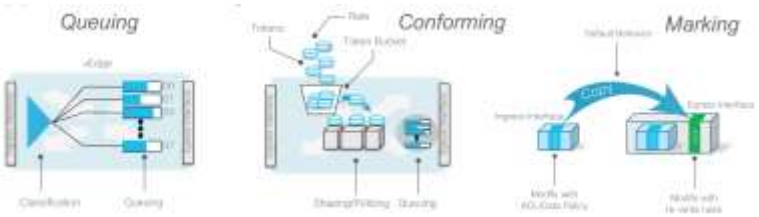
- Each vEdge advertises its local IPsec encryption key



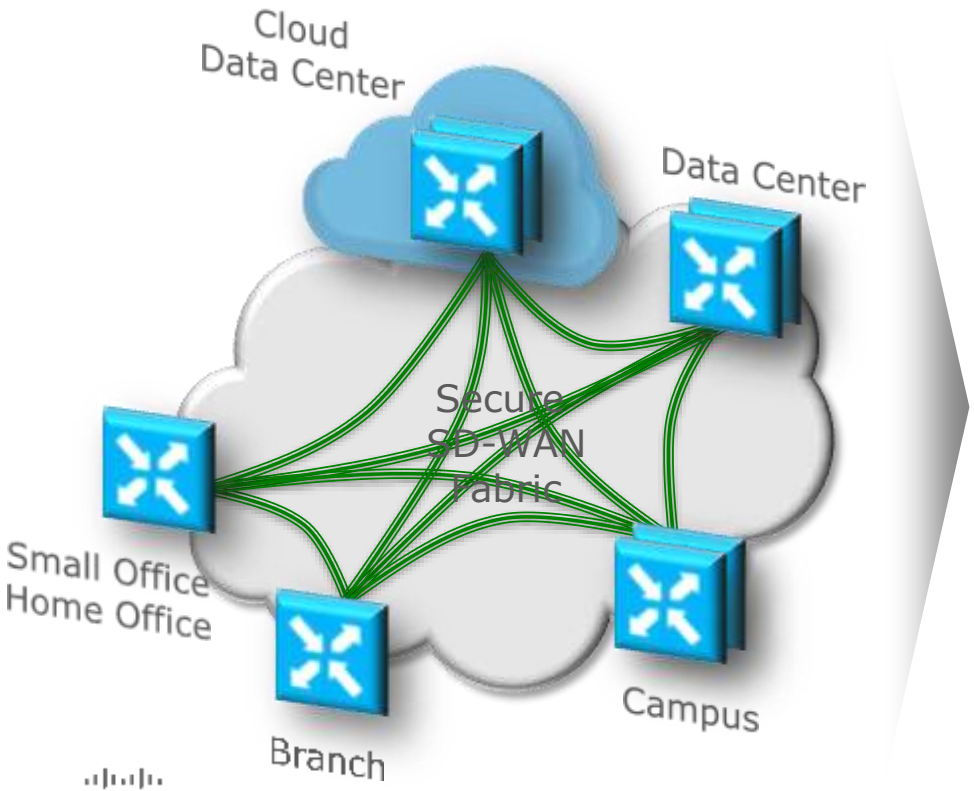
- Symmetric encryption IPsec AES256-GCM ESPv3 with HMAC SHA-1
- Traffic Encryption and Authentication Header
- Tunnel Liveliness Detection (BFD)
- Anti-Replay Protection
- Rekey **12 hours**

Application Quality of Experience

- Application Visibility
- SLA Based Policy
- Quality of Service (Queuing, Shaping and Marking)
- Application Aware Routing
- Path MTU Discovery
- Application Optimization (TCP Acceleration)
- Error Correction (FEC)



Application Visibility



Deep Packet Inspection
Over 3000+ application

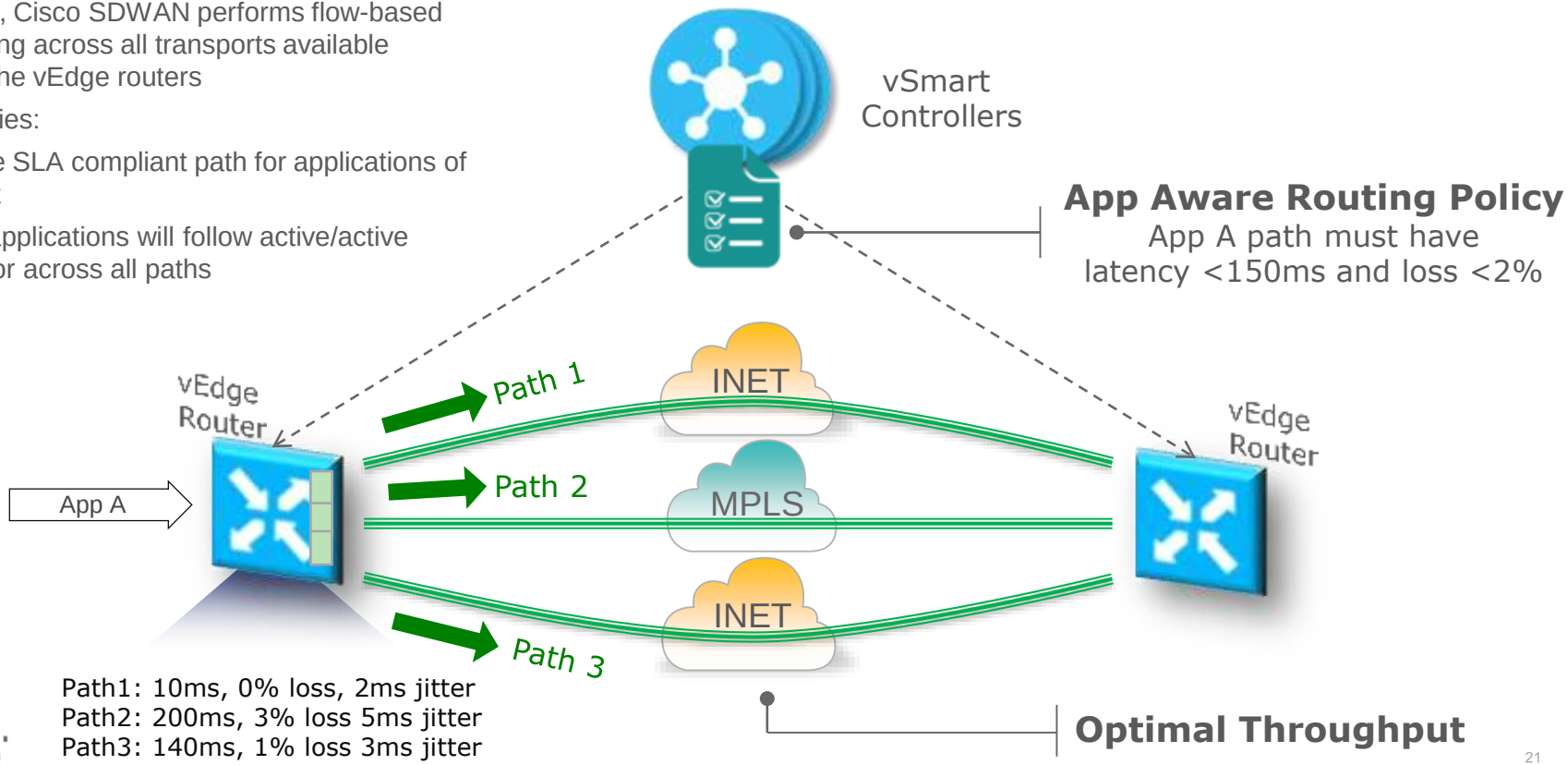
- ✓ App Firewall
- ✓ Traffic prioritization
- ✓ Transport selection

Application Performances and AAR

By default, Cisco SDWAN performs flow-based load sharing across all transports available between the vEdge routers

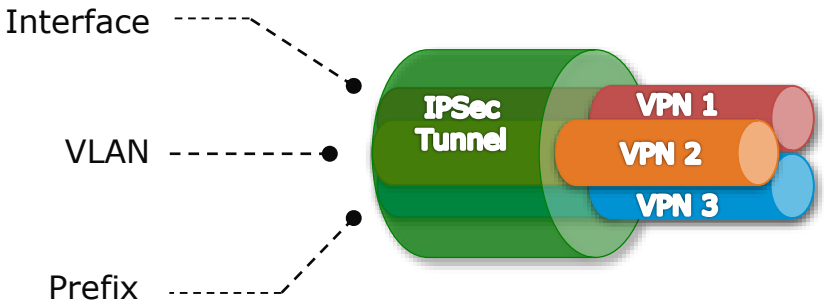
With Policies:

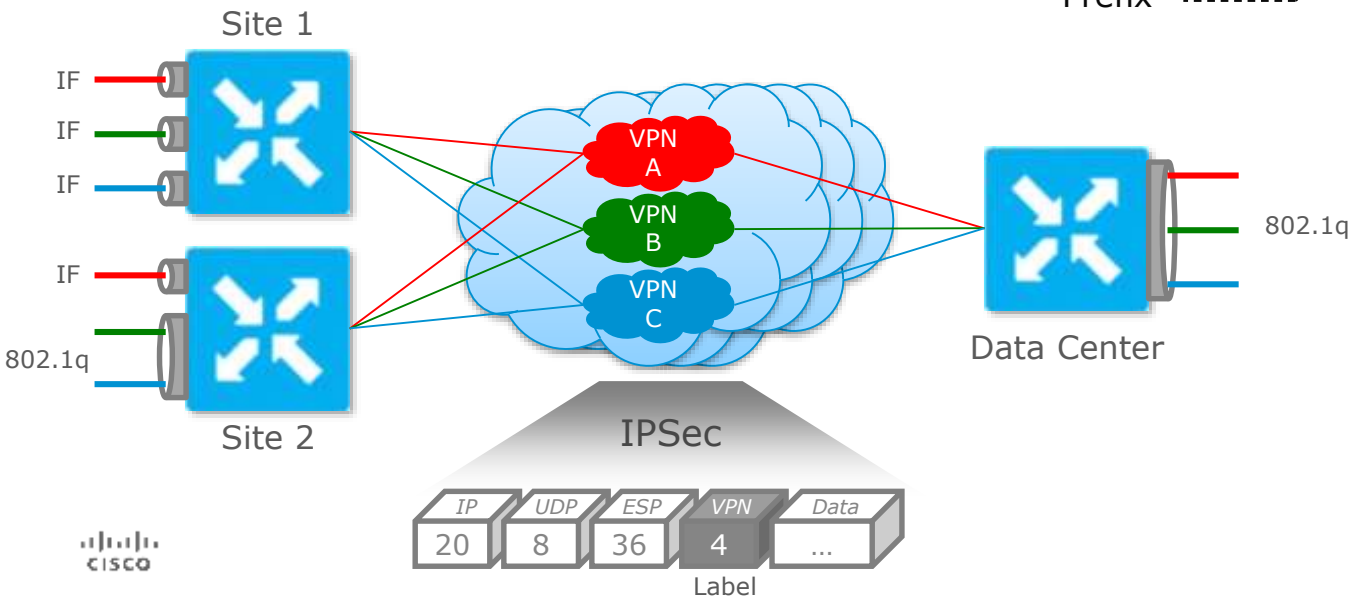
- Enforce SLA compliant path for applications of interest
- Other applications will follow active/active behavior across all paths



End to End Segmentation

- Isolated virtual private networks across any transport
- VPN mapping is based on physical vEdge Router interface, 802.1Q VLAN tag or a mix of both



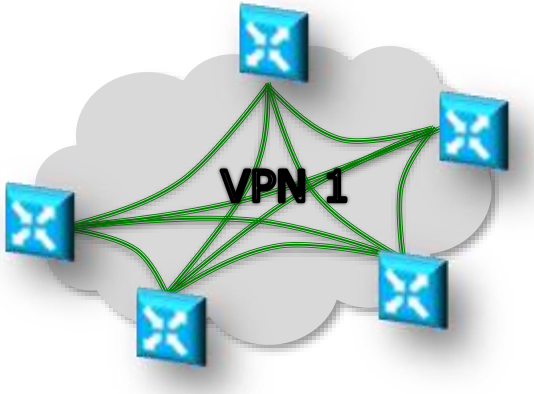


Use Cases

- Security Zoning
- Compliance
- Guest WiFi
- Multi-Tenancy
- Extranet

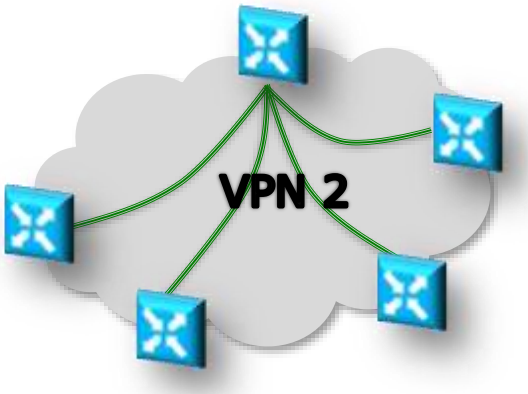
Per-Segment Topologies

Full Mesh



Unified Communications

Hub-and-Spoke



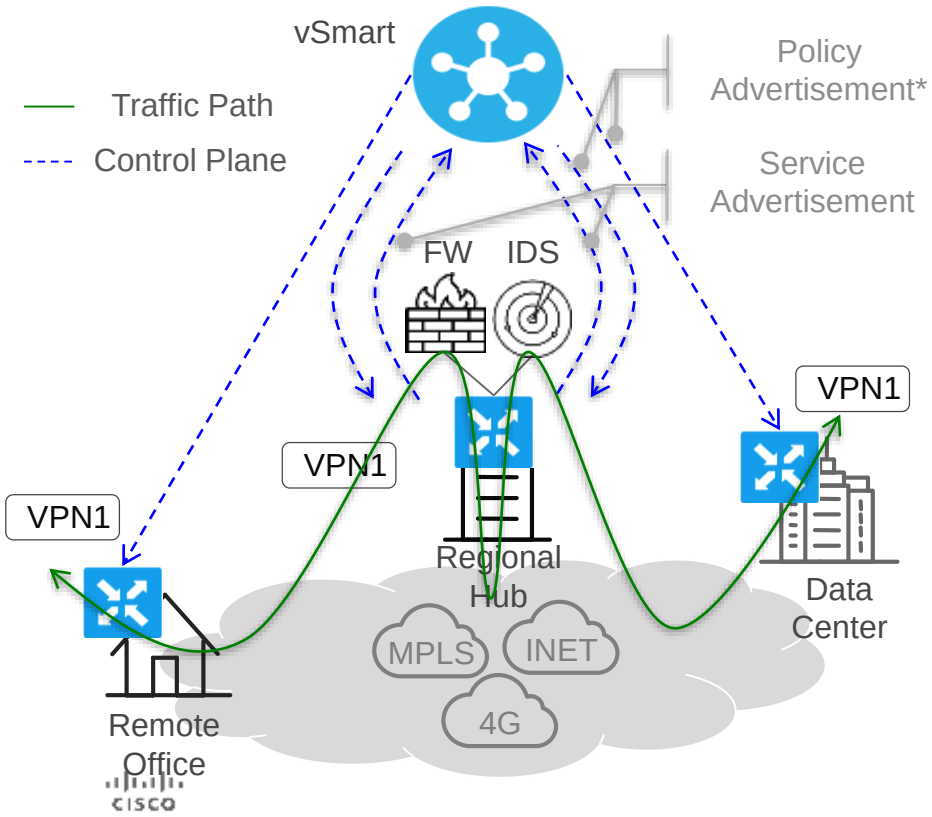
Data Center Applications

Regional Hub

Regional Internet/Services

Optimal Application Experience

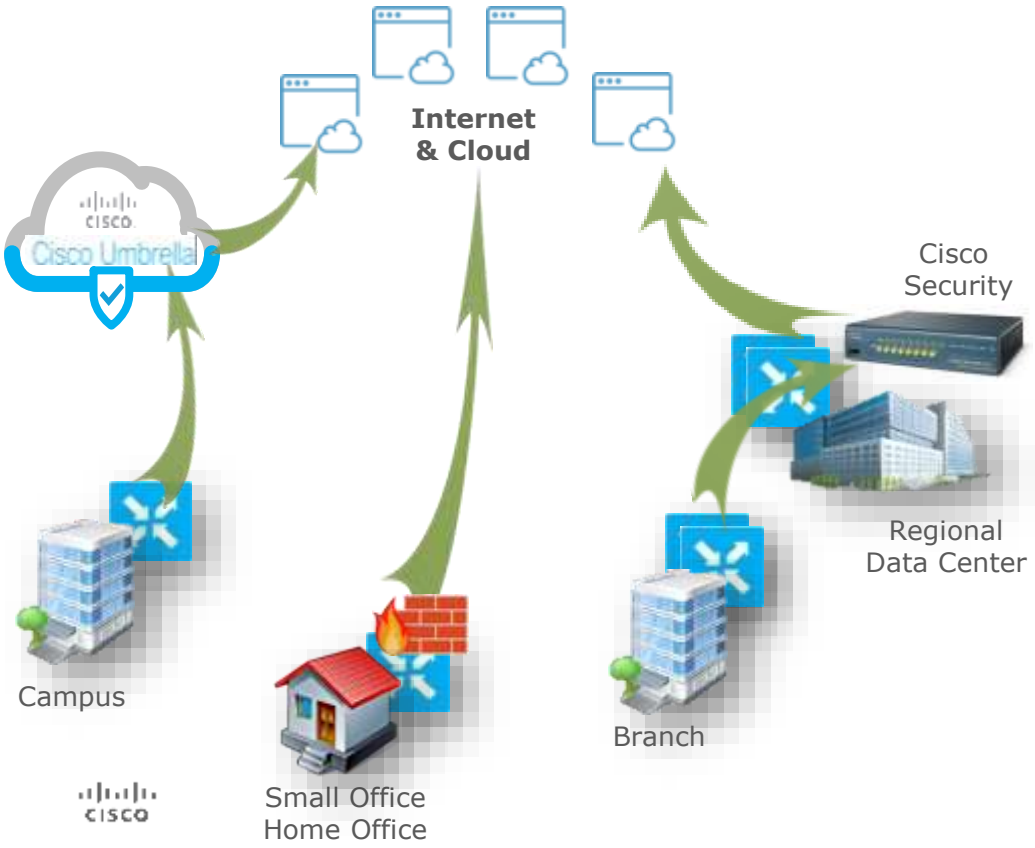
Multiple Services Chaining



- vEdge routers with connected L4-L7 service make advertisement
  - Service route OMP address family
  - Services VPN labels
- Services are advertised in specific VPN
- Services can be L3 routed or L2 bridged
- Services can be singly or dually connected to the advertising vEdges
- Control or data policies are used to insert the service nodes into the matching traffic forwarding path
  - Match on 6-tuple of DPI signature
  - Applied on ingress/egress/service vEdge

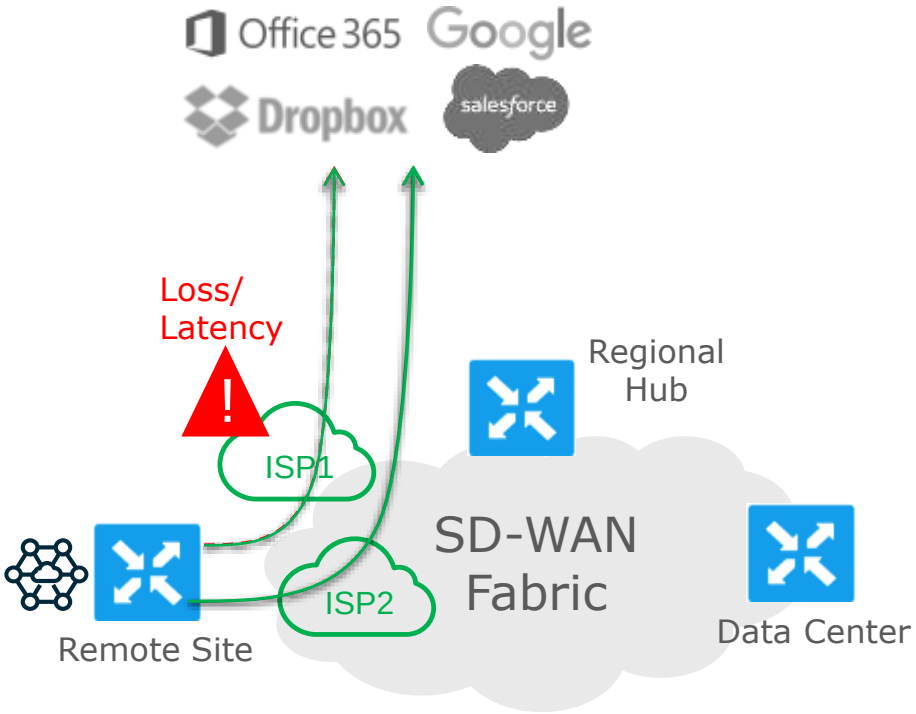
** For data policy only. Control policy enforced on vSmart.*

Secure Internet Access

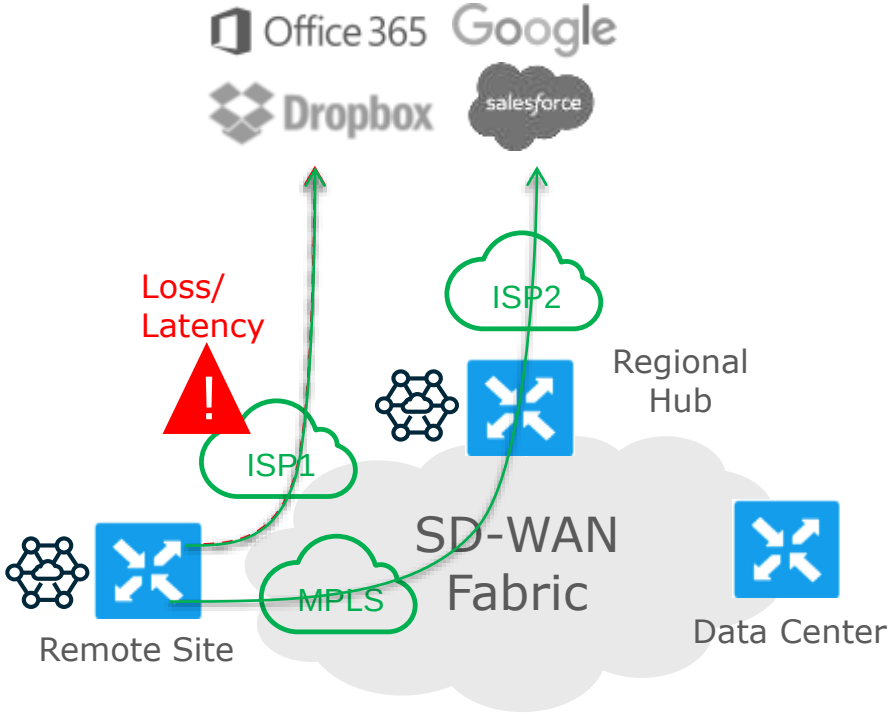


- Can use one or more local DIA exits or backhaul traffic to the regional hub through the SD-WAN fabric and exit to Internet from there
  - Per-VPN behavior enforcement
- VPN default route for all traffic DIA or data policy for selective traffic DIA
- Network Address Translation (NAT) on the vEdge router only allows response traffic back
  - Any unsolicited Internet traffic will be blocked by IP table filters
- For performance based routing toward SaaS applications use Cloud onRamp

Cloud onRamp for SaaS



Internet DIA

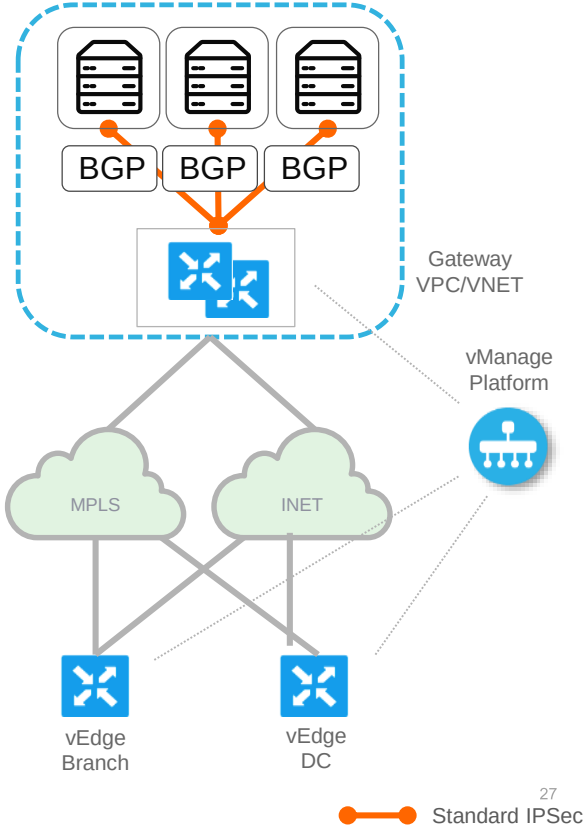


Hybrid DIA

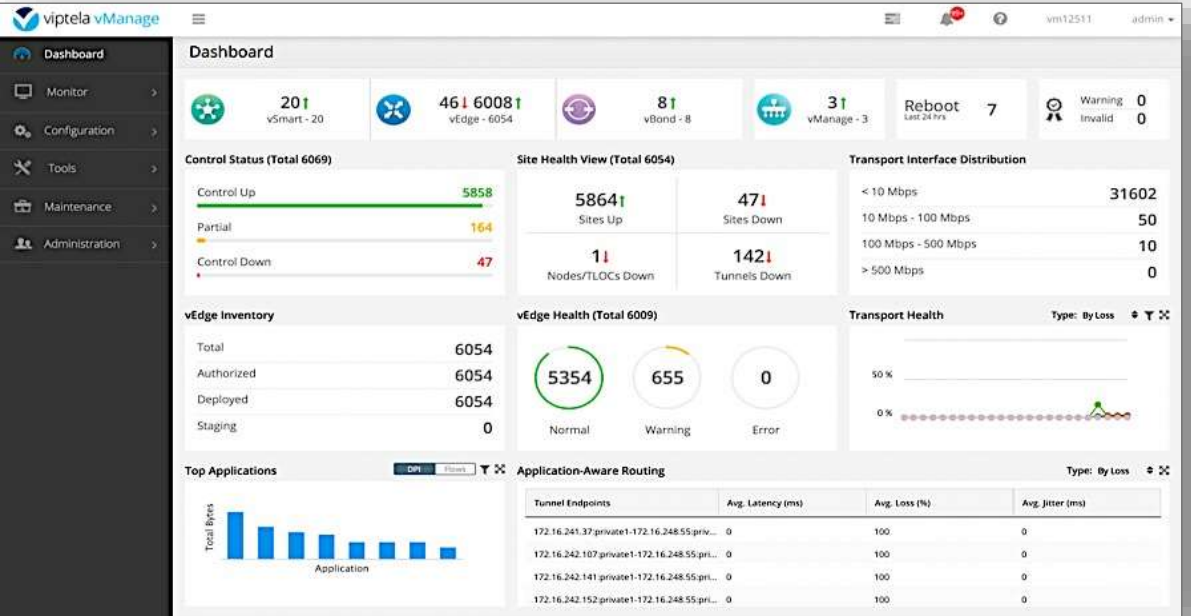
Application Quality Probing

Cloud onRamp for IaaS – Gateway VPC/VNET

- A pair of vEdge routers is instantiated in Amazon VPC or Microsoft Azure VNET
  - Gateway VPC/VNET
- A pair of standard based IPSec tunnels is stretched from gateway VPC/VNET to each host VPCs/VNETs
  - Connectivity redundancy
- BGP is established across IPSec tunnels for route advertisement
  - Bi-directional BGP/OMP redistribution on the gateway VPC/VNET vEdge routers
- Entire process is automated through vManage workflow



Centralize Management & Monitoring



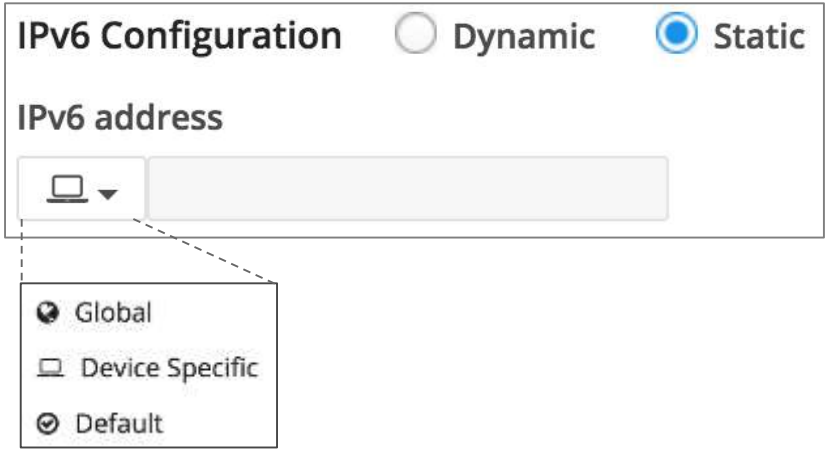
Centralize Configuration

- Security
- Template Configuration
- Policy
- Routing
- QoS, Marking
- ACL
- Application SLA
- …..

Centralize Monitoring

- Devices
- Application
- Bandwidth usage
- Link Performances
- Alerts

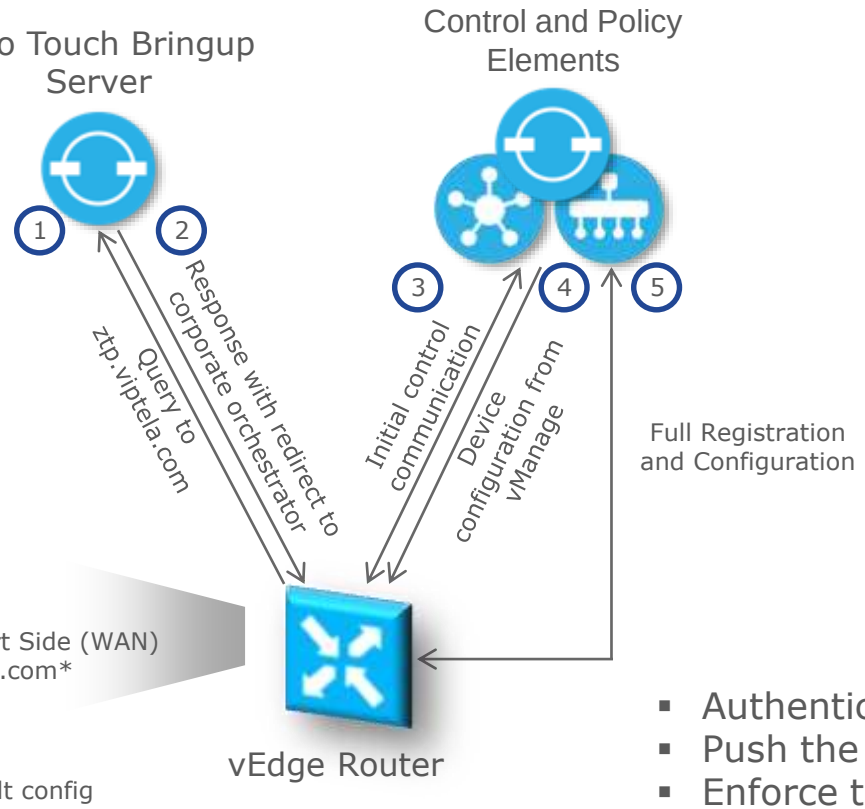
Configuration Simplicity and ZTP



- Templates are attached to provisioned vEdge routers
- Variables are used for rapid bulk configuration rollout with unique per-device settings
- Local configuration changes are not allowed
  - Prevents configuration drift

Status	Chassis Number	System IP	Hostname	Latitude	Longitude	System IP	Site ID	Bandwidth Upstream
✓	4de0b85f-a2ae-42ec-8b45-3808285cd008	1.1.1.4	RemoteSite	37.33	-121.88	1.1.1.4	104	100
✓	5f05358a-bef7-4e15-9ade-8ffd8f27ec93	1.1.1.6	AWS	45.52	-122.67	1.1.1.6	106	100
✓	9391da23-f0d1-4259-88d9-e10ae714708c	1.1.1.5	DataCenter	40.71	-74.0	1.1.1.5	105	250

Configuration Simplicity and ZTP



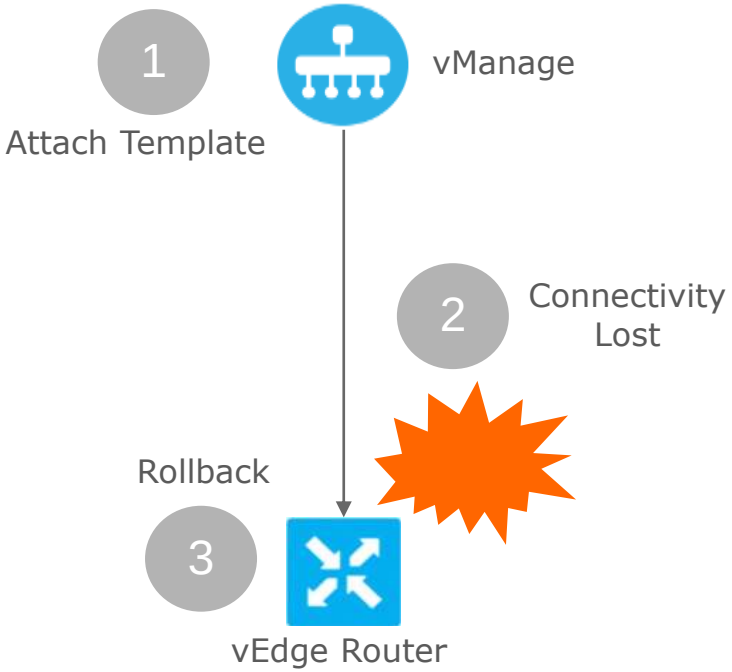
Assumption:

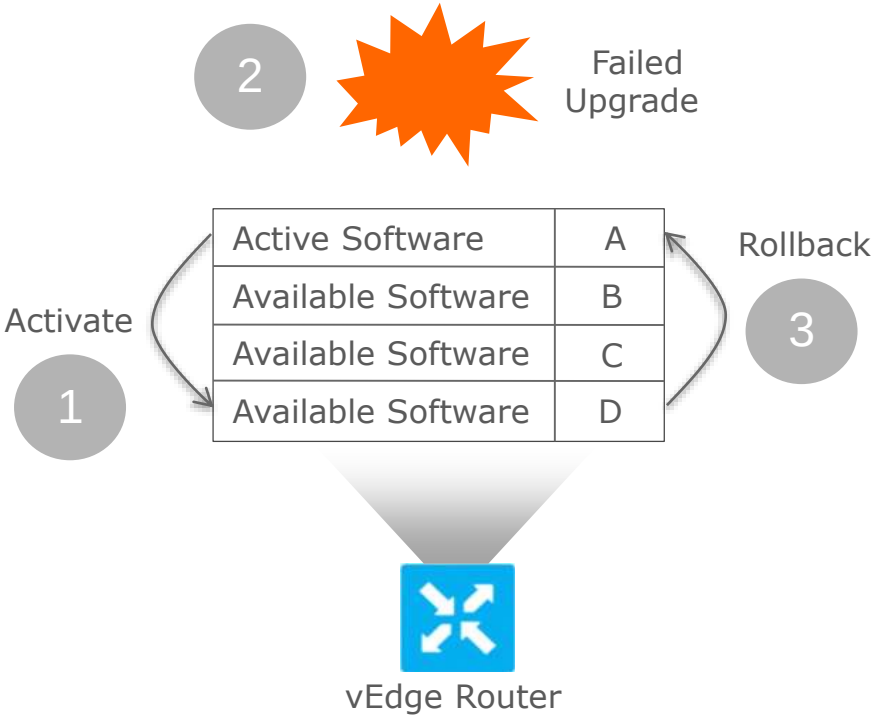
- DHCP /Stic IP on Transport Side (WAN)
- DNS to resolve ztp.viptela.com*

* Factory default config

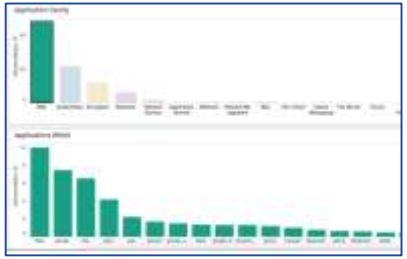
- Authentication
- Push the configuration
- Enforce the version

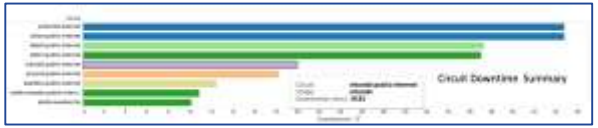
Self Healing Capabilities





Analytics Dashboard





Visibility

- Application Visibility
- Network Visibility
- Network Co-relation
- Cross-Customer Comparison

Forecast

- Application Usage Forecast
- Bandwidth Usage Forecast

What-If

- Branch Expansions
- Rolling out new applications
- Policy changes

Recommendation

Why Cisco SD-WAN

Trusted by Fortune 800 Enterprises

Viptela SEN: The Most-Deployed Enterprise Grade SD-WAN
Thousands of sites, every major industry, including:

Standards Compliant: HIPAA PCI …and more

Most deployed and trusted by Fortune 500 enterprises

Winning 95% of competitive POCs

CISCO

TOMORROW starts here.